UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,943	03/07/2005	Carl Gustavsson	9562-9	8802

20792   7590   01/28/2009
MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER
PHAM, LUU T

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
01/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 January 2009*.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *46-75* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *46-75* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application

is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37

CFR 1.17(e) has been timely paid, the finality of the previous Office action has been

withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/07/2009 has

been entered.

2.   As per instant Amendment, Claims 1-45 were previously canceled; Claims 46, 59, and 69

are independent claims. Claims 46-75 have been examined and are pending.

This Action is made Non-FINAL.

Response to Arguments

3.   Applicants' arguments in the instant Amendment, filed on 01/07/2009, have been fully

considered but they are not persuasive.

   Applicants' arguments:

   a.   *"SyncML does not disclose or suggest 'incorporating into a message the*

authentication method indicator comprising a plurality of authentication

capabilities of the communication apparatus __among the plurality of different__

__authentication methods__,' as recited in Claim 46, as amended."

b. *"The cited portions of SyncML that are interpreted as disclosing 'the authentication method indicator' are included in packages from the server to the apparatus and not vice versa."*

The Examiner disagrees due to the following reasons:

a. SyncML does disclose incorporating into a message the authentication method indicator *(pages 20-27; section 3.5.1; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-basic>; section 3.5.2; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-md5>; section 4.1.1; page 13, section 2.5; both the sync client and server can challenge for the authentication and the device receiving the authentication challenge must be able to send the authorization credentials back; see also pages 26-30 and 34-40)* comprising a plurality of authentication capabilities of the communication apparatus *(page 13, section 2.5; the protocol requires the support for the basic authentication and the MD5 digest access authentication; pages 21-27, section 3.5.1; XML Tag 'type' <auth-basic>; XML Tag 'type' <auth-md5>; client and server is able to perform authentication using either auth-basic or auth-MD5; see also pages 26-30 and 34-40)* among the plurality of different authentication methods *(pages 20-27; auth-basic and auth-MD5 are known as plurality of different authentication methods)*.

b. SyncML the authentication method indicator is included in the packages sent to the server from the client *(pages 20-27; section 3.5.1; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-basic>; section 3.5.2; Pkg #1 (with*

credentials) from client; XML Tag 'type' <auth-md5>; section 4.1.1: 'Example of

Sync Initialization of Packet from Client'; XML Tag 'type' <auth-basic>).

Claim Objections

4.   The amendment filed 01/07/2009 is objected to under 35 U.S.C. 132(a) because it introduces

new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new

matter into the disclosure of the invention. The added material which is not supported by the

original disclosure is as follows: Claims 46, 59, and 69 recite the limitation *"a **subset** comprises*

***addition authentication methods**,"* (emphasis added). However, the aforementioned limitation is

not discussed in the specification.

The Examiner respectfully requests the Applicant to point out where in the

specification support can be found for the aforementioned newly added limitations.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 101

5.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter,
> or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
> requirements of this title.

6.   **Claims 59-75 are rejected under 35 U.S.C. 101** as being directed to non-statutory

subject matter.

- **Regarding claim 59**, the claim is not directed to eligible subject matter in view of *In re Comiskey*, 499 F.3d 1365 (Fed. Cir. 2007). Although the preamble of the claim recites *"an electronic communication apparatus,"* the body of the claim does not positively recite any elements of hardware. The claim merely recites *"means for synchronizing,"* *"means for providing an authentication method,"* and *"means for incorporating,"* and does not positively recite any element of hardware or machine (e.g., a computer) that the aforementioned means for are tied to. There is no further disclosure in the specification as to how the aforementioned *"means for"* are implemented. Therefore, the nature of the subject matter claimed may reasonably be construed as a mental process since the language of claim 59 broadly encompasses non-tangible embodiments. See *In Re Bilski*, 88 USPQ2d 1385; see also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 473 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1976)); The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101.

- **Regarding claims 60-68**, claims 60-68 are also directed to non-statutory subject matter for the same reasons.

- **Regarding claim 69**, the claim is not directed to eligible subject matter in view of *In re Comiskey*, 499 F.3d 1365 (Fed. Cir. 2007). Although the preamble of the claim recites *"a server,"* the body of the claim does not positively recite any elements of hardware. The claim merely recites *"means for incorporating,"* and *"means for*

determining," and does not positively recite any element of hardware or machine (e.g., a

computer) that the aforementioned means for are tied to. There is no further disclosure in

the specification as to how the aforementioned *"means for"* are implemented. Therefore,

the nature of the subject matter claimed may reasonably be construed as a mental process

since the language of claim 69 broadly encompasses non-tangible embodiments. See *In Re*

Bilski, 88 USPQ2d 1385; see also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v.*

Flook, 473 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972);

Cochrane v. Deener, 94 U.S. 780, 787-88 (1976)); The mere recitation of the machine in

the preamble with an absence of a machine in the body of the claim fails to make the claim

statutory under 35 USC 101.

- **Regarding claims 70-75**, claims 70-75 are also directed to non-statutory subject

matter for the same reasons.

Claim Rejections - 35 USC § 112

7.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming
> the subject matter which the applicant regards as his invention.

8.   **Claims 59-75 are rejected under 35 U.S.C. 112, second paragraph,** as being indefinite.

- **Regarding claims 59-60, 62-64, 69, 70, and 72**; claims 59-60, 62-64, 69, 70,

and 72 have been found in valid as indefinite because the claims recite *"means for"*

languages and there is no structure disclosed in the specification. *"If there is no structure in*

the specification corresponding to the means-plus-function limitation in the claims, the

claims will be found invalid as indefinite." Biomedino, LLC vs. Waters Technology Corp.,
490 F.3d 946, 950 (Fed. Cir. 2007)

- **Regarding claims 61, 65-68, 71, 73, and 74-75**; claims 61, 65-68, 71, 73, and

74-75 are dependent on either claim 59 or 69, and therefore inherit the 35 U.S.C 112,

second paragraph issues of the independent claims.

Claim Rejections - 35 USC § 102

9.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or
> on sale in this country, more than one year prior to the date of application for patent in the United States.

10.   **Claims 46-49, 54-56, 59-62, and 67-71 are rejected under 35 U.S.C. 102(b)** as being

anticipated by "SyncML Sync Protocol, version 1.0," (hereinafter "SyncML"), SYNCML

CONSORTIUM, published on December 07, 2000.

- **Regarding claim 46**, SyncML discloses a method for providing authentication

when messages are sent between an electronic communication apparatus and a server

according to a synchronization protocol *(page 8, Fig. 2; page 20, section 3: authentication)*

in which a plurality of different authentication methods, among which a subset comprises

addition authentication methods *(pages 20-27; auth-basic and auth-MD5 are known as*

plurality of different authentication methods), comprising:

providing an authentication method indicator *(pages 20-27, sections 3.5 and 4.1;*

XML Tag 'type'; see also page 13, section 2.5) that specifies an authentication method of

the plurality of different authentication methods *(pages 20-27; auth-basic and auth-MD5*

are known as plurality of different authentication methods) according to which the

authentication is to be executed *(page 20, section 3; page 21, section 3.5; XML Tag*

'SyncML' and 'VerDTD');

incorporating into a message the authentication method indicator *(pages 20-27;*

section 3.5.1; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-basic>; section

3.5.2; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-md5>; section 4.1.1;

page 13, section 2.5; both the sync client and server can challenge for the authentication

and the device receiving the authentication challenge must be able to send the

authorization credentials back; see also pages 26-30 and 34-40) comprising a plurality of

authentication capabilities of the communication apparatus *(page 13, section 2.5; the*

protocol requires the support for the basic authentication and the MD5 digest access

authentication; pages 21-27, section 3.5.1; XML Tag 'type' <auth-basic>; XML Tag 'type'

<auth-md5>; see also pages 26-30 and 34-40) among the plurality of different

authentication methods *(pages 20-27; auth-basic and auth-MD5 are known as plurality of*

different authentication methods); and

transmitting said message to said server according to an authentication protocol

of the synchronization protocol *(page 22; Pkg #1 (with credentials) from client; data inside*

XML Tag 'type'<auth-basic>; page 23; Pkg #1 (with credentials from Client; syncML:

<auth-md5>; see also page 27; section 4.1.1: 'Example of Sync Initialization of Packet

from Client').

- **Regarding claim 47**, SyncML discloses the method according to claim 46,

wherein the authentication method indicator is incorporated into a meta command of the

synchronization protocol *(page 22, Pkg #1 (with credentials) from Client; XML Tag 'Meta'*

includes <auth-basic>; page 23; Pkg #1 (with credentials) from Client; see also page 27;

section 4.1.1: 'Example of Sync Initialization of Packet from Client').

- **Regarding claim 48**, SyncML discloses the method according to claim 46,

wherein the message is an initialization message *(pages 22-25; Pkg #1 (with credentials)*

from Client; Fig. 6; Pkg #1: client initialization package to server), and the authentication

capabilities of the electronic communication apparatus is indicated in an authentication

method list of the initialization message *(page 15, section 2.7; pages 22-24, section 3.5;*

pages 25-27, section 4), which is sent to the server for establishing a connection *(page 25;*

Fig. 6; Pkg #1: client initialization package to server).

- **Regarding claim 49**, SyncML discloses the method according to claim 46,

wherein any authentication data relating to the specified authentication method is

incorporated in a data string of the message-sent according to the synchronization protocol

(page 21, section 3.5; the client sends Pkg #1 with the credentials; the server accepts the

credentials and the session is authenticated; see also page 25; Fig. 6).

- **Regarding claim 54**, SyncML discloses the method according to claim 48, further comprising: determining at the server the authentication capabilities of the electronic communication apparatus based on the plurality of authentication capabilities listed in the authentication method list *(page 20, section 3.1-3.3; page 21, section 3.5.1; the client sends Pkg #1 with credentials; the server accepts the credentials and the session is authenticated; see also pages 22-23; Pkg #1 (with credentials) from Client; information inside XML Tag 'type' includes <auth-basic> and <auth-md5>).*

- **Regarding claim 55**, SyncML discloses the method according to claim 54, further comprising:

    executing at the server authentication operations according to one of the plurality of authentication capabilities indicated in the authentication method list *(page 21, section 3.5; the client sends Pkg #1 with the credentials; the server accepts the credentials and the session is authenticated; see also page 25; Fig. 6)*;

    preparing a message at the server comprising the authentication method indicator and any authentication data relating to the specified authentication method *(pages 21-23; see Pkg #2 from server)*; and

    transmitting the message to the electronic communication apparatus *(page 25, Fig. 6; Pkg #2: server initialization package to client)*.

- **Regarding claim 56**, SyncML discloses the method according to claim 55, further comprising:

receiving the message at the electronic communication apparatus *(page 25; Fig. 6; server initialization package to client)*;

executing, at the electronic communication apparatus, authentication operations according to the authentication method indicated by the authentication method indicator to generate an expected result *(page 21, section 3.5; the client sends Pkg #1 with the credentials; the server accepts the credentials and the session is authenticated; see also page 25; Fig. 6)*;

preparing a response to the server comprising the authentication method indicator, and any authentication data *(page 26, section 4.1; initialization requirements for client; see also page 33; Fig. 7; client makes data update for its databases)*; and

transmitting the response to the server *(page 26, section 4.1; initialization requirements for client; see also page 33; Fig. 7; client sends server Pkg #5, data update status package)*.

- **Regarding claim 59**, SyncML discloses an electronic communication apparatus, comprising:

means for synchronizing via a synchronization *(page 7; section 1.1; Fig. 1; wherein at least boxes: 'Sync Server Agent' and 'Sync Client Agent')* , protocol in which a plurality of different authentication methods are available, among which a subset comprises addition authentication *(pages 20-27; section 3.5.1; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-basic>; section 3.5.2; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-md5>; section 4.1.1auth-basic and auth-MD5 are known as plurality of different authentication method)* methods;

means for providing an authentication method indicator *(pages 20-27, sections 3.5 and 4.1; XML Tag 'type'; see also page 13, section 2.5)* that specifies an authentication method of the plurality of different authentication methods according to which the authentication is to be executed *(pages 20-27; sections 3.5.1, 3.5.2, and 4.1.1; auth-basic and auth-MD5 are known as plurality of different authentication method)*;

means for incorporating into a message the authentication method indicator *(pages 20-27; section 3.5.1; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-basic>; section 3.5.2; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-md5>; section 4.1.1; page 13, section 2.5; both the sync client and server can challenge for the authentication and the device receiving the authentication challenge must be able to send the authorization credentials back; see also pages 26-30 and 34-40)* comprising a plurality of authentication capabilities of the communication apparatus *(page 13, section 2.5; the protocol requires the support for the basic authentication and the MD5 digest access authentication; pages 21-27, section 3.5.1; XML Tag 'type' <auth-basic>; XML Tag 'type' <auth-md5>; see also pages 26-30 and 34-40)* among the plurality of different authentication methods *(pages 20-27; auth-basic and auth-MD5 are known as plurality of different authentication methods)*; and

means for transmitting said message to a server according to an authentication protocol of the synchronization protocol *(page 22; Pkg #1 (with credentials) from client; data inside XML Tag 'type'<auth-basic>; page 23; Pkg #1 (with credentials from Client; syncML: <auth-md5>; see also page 27; section 4.1.1: 'Example of Sync Initialization of Packet from Client')*;

- **Regarding claim 60**, SyncML discloses the electronic communication apparatus according to claim 59, further comprising: means for sending an initialization message to the server for establishing a connection, the message comprising the authentication method indicator *(pages 22-25; Pkg #1 (with credentials) from Client; Fig. 6; Pkg #1: client initialization package to server)*.

- **Regarding claim 61**, SyncML discloses the electronic communication apparatus according to claim 60, wherein the initialization message further comprises type of apparatus and/or identity of the electronic communication apparatus *(pages 27-28, section 4.1.1; XML Tags 'PropName' includes <TEL>, <VOICE>, and <CELL>; see also page 31; XML Tags 'PropName')*.

- **Regarding claim 62**, SyncML discloses the electronic communication apparatus according to claim 61, further comprising: means for incorporating authentication data in a data string of the message to be sent according to the synchronization protocol *(page 21, section 3.5; the client sends Pkg #1 with the credentials; the server accepts the credentials and the session is authenticated; see also page 25; Fig. 6)*.

- **Regarding claim 67**, SyncML discloses the electronic communication apparatus according to claim 59, wherein the electronic communication apparatus is a pager, an electronic organizer, and/or a smartphone *(page 8, section SyncML Client; the SyncML client is typically a mobile phone, PC, or PDA device; see also Fig. 2; synchronization example with mobile phone and server)*.

- **Regarding claim 68**, SyncML discloses the electronic communication apparatus according to claim 59, wherein the electronic communication apparatus is a mobile telephone *(page 8; Fig. 2; synchronization example with mobile phone and server)*.

- **Regarding claim 69**, SyncML discloses a server for synchronizing by a synchronization protocol *(page 7; section 1.1; Fig. 1; wherein at least boxes: 'Sync Server Agent' and 'Sync Client Agent')* in which a plurality of different authentication methods are available, among which a subset comprises addition authentication method *(pages 20-27; section 3.5.1; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-basic>; section 3.5.2; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-md5>; section 4.1.1; auth-basic and auth-MD5 are known as plurality of different authentication method)*, the server comprising:

    means for incorporating an authentication method indicator in a message to be sent *(pages 20-27; section 3.5.1; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-basic>; section 3.5.2; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-md5>; section 4.1.1; page 13, section 2.5; both the sync client and server can challenge for the authentication and the device receiving the authentication challenge must be able to send the authorization credentials back; see also pages 26-30 and 34-40)* according to an authentication protocol of a synchronization protocol *(page 7; section 1.1; Fig. 1; wherein at least boxes: 'Sync Server Agent' and 'Sync Client Agent')* for indicating an authentication method of the plurality of different authentication methods according to which the authentication is to be executed *(pages 20-27; sections 3.5.1, 3.5.2, and 4.1.1; XML Tag 'type'; <auth-basic> and <auth-MD5>)*;

means for determining from the authentication method indicator of a received

message, a plurality of authentication capabilities of an apparatus among the plurality of

different authentication methods *(pages 20-27; section 3.5.1; Pkg #1 (with credentials)*

from client; XML Tag 'type' <auth-basic>; section 3.5.2; Pkg #1 (with credentials) from

client; XML Tag 'type' <auth-md5>; section 4.1.1; auth-basic and auth-MD5 are known

as plurality of different authentication method); and

electronic apparatus for determining the authentication method to use based on

the plurality of authentication capabilities *(pages 20-27, section 3.1-3.3; section 3.5.1;*

XML Tag 'type'; <auth-basic> and <auth-MD5>; the client sends Pkg #1 with

credentials; the server accepts the credentials and the session is authenticated).

- **Regarding claim 70**, is similar in scope to claim 62, and is therefore rejected

under similar rationale.

- **Regarding claim 71**, SyncML discloses the server according to claim 69,

further comprising: means for executing authentication according to the determined

authentication method *(page 21, section 3.5; the client sends Pkg #1 with the credentials;*

the server accepts the credentials and the session is authenticated; see also page 25; Fig.

6).

Claim Rejections - 35 USC § 103

11.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title, if the differences between the subject matter sought to be patented and

> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

12.   This application currently names joint inventors. In considering patentability of the claims

under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various

claims was commonly owned at the time any inventions covered therein were made absent

any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to

point out the inventor and invention dates of each claim that was not commonly owned at

the time a later invention was made in order for the examiner to consider the applicability

of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C.

103(a).

13.   **Claims 50-51, 57, 63-65, and 72-74 are rejected under 35 U.S.C. 103(a)** as being

unpatentable over SyncML, as applied to claims 46, 59, and 69 above, and further in view

of Quick, Jr. et al., (hereinafter "Quick"), U.S. Patent Application No. 2002/0091933, filed

on May 22, 2001.

- **Regarding claim 50**, SyncML discloses the method according to claim 46.

  SynnML does not explicitly disclose the authentication method is Global System

for Mobile communication (GSM) Subscriber Identify Module (SIM) authentication.

  However, in an analogous art, Quick discloses a method for providing local

authentication, wherein the authentication method is Global System for Mobile

communication (GSM) Subscriber Identify Module (SIM) authentication *(Quick: pars.*

0005-0006; Subscriber Identity Module (SIM) is used in GSM system; an authentication

key for identifying the subscriber).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to combine the method and system of Quick with that of

SyncML wherein the authentication method is Global System for Mobile communication

(GSM) Subscriber Identify Module (SIM) authentication to allows a subscriber to travel

without his or her personal mobile phone and to use locally available mobile phone without

incurring costs in establishing a new account *(Quick: par. 0005)*.

- **Regarding claim 51**, SyncML discloses the method according to claim 46.

    SyncML does not explicitly disclose the authentication method is Universal

Mobile Telephone System (UMTS) Universal Subscriber Identity Module (USIM)

authentication, which provides server authentication.

    However, in an analogous art, Quick discloses a method for providing local

authentication, wherein the authentication method is Universal Mobile Telephone System

(UMTS) Universal Subscriber Identity Module (USIM) authentication, which provides

server authentication *(Quick: pars. 0005 and 0006; next generation SIM card have been*

renamed as USIM used in UTMS system; an authentication key for identifying the

subscriber).

    Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to combine the method and system of Quick with that of

SyncML wherein the authentication method is Universal Mobile Telephone System

(UMTS) Universal Subscriber Identity Module (USIM) authentication, which provides

server authentication to allows a subscriber to travel without his or her personal mobile

phone and to use locally available mobile phone without incurring costs in establishing a

new account *(Quick: par. 0005)*.

- **Regarding claim 57**, SyncML discloses the method according to claim 46.

SyncML does not explicitly disclose the authentication method is Subscriber

Identify Module/Universal Subscriber Identify Module (SIM/USIM) authentication, the

method further comprising: using CKs/IKs (cipher keys/integrity keys) generated by the

electronic communication apparatus and the server, respectively, to provide integrity

protection, wherein the CKs/IKs are used for generating MAC values; and using a hashing

function for computing a Hashed Method Authentication Code (HMAC) on the message.

However, in an analogous art, Quick discloses a method for providing local

authentication, wherein the authentication method is Subscriber Identify Module/Universal

Subscriber Identify Module (SIM/USIM) authentication, the method further comprising:

using CKs/IKs (cipher keys/integrity keys) generated by the electronic communication

apparatus and the server, respectively, to provide integrity protection *(Quick: pars. 0024*

and 0026-0027; cipherkey 290 and integrity key 310), wherein the CKs/IKs are used for

generating MAC values *(Quick: pars. 0026; the IK 310 can be used to generate a message*

authentication code MAC); and using a hashing function for computing a Hashed Method

Authentication Code (HMAC) on the message *(Quick: par. 0038; HMAC-SHA-1 scheme;*

HMAC is implemented in the subscriber identification token).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to combine the method and system of Quick with that of

SyncML wherein the authentication method is Subscriber Identify Module/Universal

Subscriber Identify Module (SIM/USIM) authentication, the method further comprising:

using CKs/IKs (cipher keys/integrity keys) generated by the electronic communication

apparatus and the server, respectively, to provide integrity protection, wherein the CKs/IKs

are used for generating MAC values; and using a hashing function for computing a Hashed

Method Authentication Code (HMAC) on the message to provide users with a mean for

providing secure authentication to a subscriber roaming outside his or her home system

(Quick: par. 0007).

- **Regarding claim 63**, SyncML discloses the electronic communication apparatus

according to claim 59.

SyncML does not explicitly disclose means for using an IK (integrity key) to

generate a MAC to provide integrity protection; and means for using a hashing function to

compute a Hashed Method Authentication Code (HMAC) on the message to be sent.

However, in an analogous art, Quick discloses a method for providing local

authentication, wherein means for using an IK (integrity key) to generate a MAC to

provide integrity protection *(Quick: pars. 0026; the IK 310 can be used to generate a*

message authentication code MAC); and means for using a hashing function to compute a

Hashed Method Authentication Code (HMAC) on the message to be sent *(Quick: par.*

0038; HMAC-SHA-1 scheme; HMAC is implemented in the subscriber identification

token).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to combine the method and system of Quick with that of

SyncML wherein means for using an IK (integrity key) to generate a MAC to provide

integrity protection; and means for using a hashing function to compute a Hashed Method

Authentication Code (HMAC) on the message to be sent to provide users with a mean for

providing secure authentication to a subscriber roaming outside his or her home system

(Quick: par. 0007).

- **Regarding claim 64**, claim 64 is similar in scope to claim 50, and is therefore
rejected under similar rationale.

- **Regarding claim 65**, claim 65 is similar in scope to claim 51, and is therefore
rejected under similar rationale.

- **Regarding claim 72**, claim 72 is similar in scope to claim 63, and is therefore
rejected under similar rationale

- **Regarding claim 73**, claim 73 is similar in scope to claim 50, and is therefore
rejected under similar rationale.

- **Regarding claim 74**, claim 74 is similar in scope to claim 51, and is therefore
rejected under similar rationale.

14. **Claims 52 and 66 are rejected under 35 U.S.C. 103(a)** as being unpatentable over

SyncML, as applied to claims 46 and 59 above, and further in view of Lahteenmaki, U.S.

Patent Application No. 2003/0028805, filed on August 03, 2001.

- **Regarding claim 52**, SyncML discloses the method according to claim 46.

SyncML does not explicitly disclose the authentication method is WPKI or WIM authentication.

However, in an analogous art, Lahteenmaki discloses a method for managing network service access and enrolment, wherein the authentication method is WPKI or WIM authentication *(Lahteenmaki: par. 0038; WAP Public key Infrastructure (WPKI) provides a manner of enabling the trust relationships needed for authentication of servers and clients)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Lahteenmaki with that of SyncML wherein the authentication method is WPKI or WIM authentication to provide users with a means for managing user access and enrollment for secure network services *(Lahteenmaki: par. 0001)*.

- **Regarding claim 66**, claim 66 is similar in scope to claim 52, and is therefore rejected under similar rationale.

15. **Claims 53 and 75 are rejected under 35 U.S.C. 103(a)** as being unpatentable over SyncML, as applied to claims 46, 59, and 69 above, and further in view of Tran et al., (hereinafter "Tran"), U.S. Patent Application No. 2003/0033524, filed on August 13, 2001.

- **Regarding claim 53**, SyncML the method according to claim 46.

SyncML does not explicitly disclose the authentication method is SecureId or SafeWord authentication.

However, in an analogous art, Tran discloses a wireless portal system, wherein the authentication method is SecureId or SafeWord authentication *(Tran: par. 0052; the authentication modules may also include LDAP authentication, secure ID, radius authentication, etc.)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Tran with that of SyncML wherein the authentication method is SecureId or SafeWord authentication to provide access to any type of service from any type of device from anywhere and to provide content suitable for these devices without incurring substantial cost overhead *(Tran: par. 0008)*.

- **Regarding claim 75**, SyncML discloses the server according to claim 69.

SyncML does not explicitly disclose the authentication method is SecureId, SafeWord, Wireless Public Key Infrastructure (WPKI) and/or Wireless Identity Module (WIM) authentication.

However, in an analogous art, Tran discloses a wireless portal system, wherein the authentication method is SecureId, SafeWord, Wireless Public Key Infrastructure (WPKI) and/or Wireless Identity Module (WIM) authentication *(Tran: par. 0052; the authentication modules may also include LDAP authentication, secure ID, radius authentication, etc.)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Tran with that of SyncML wherein the authentication method is SecureId, SafeWord, Wireless Public Key

Infrastructure (WPKI) and/or Wireless Identity Module (WIM) authentication to provide

access to any type of service from any type of device from anywhere and to provide

content suitable for these devices without incurring substantial cost overhead *(Tran: par.*

0008).

16.   **Claim 58 is rejected under 35 U.S.C. 103(a)** as being unpatentable over SyncML and

Lahteenmaki, as applied to claim 52 above, and in view of Quick, Jr. et al., (hereinafter

"Quick"), U.S. Patent Application No. 2002/0091933, filed on May 22, 2001, and further

in view of Beatson, U.S. Patent Application No. 2003/0056100, filed on September 14,

2001.

- **Regarding claim 58**, SyncML and Lahteenmaki disclose the method according

to claim 52.

SyncML and Lahteenmaki do not explicitly disclose generating, at the server, an

integrity key that is encrypted with the public key of the electronic communication

apparatus; sending the integrity key to the electronic communication apparatus; using the

integrity key at the electronic communication apparatus to generate MAC values; and using

a hashing function at the electronic communication apparatus to compute a Hashed Method

Authentication Code (HMAC) on the message.

However, in an analogous art, Quick discloses a method for providing local

authentication, wherein generating, at the server, an integrity key *(Quick: par. 0024; key*

generator 250 generates a cryptographic cipher key (CK) 290 and an integrity key (IK)

310);

sending the integrity key to the electronic communication apparatus *(Quick: pars. 0024 and 0026-0027; IK 310 is conveyed to the mobile unit 220)*;

using the integrity key at the electronic communication apparatus to generate MAC values *(Quick: pars. 0026; the IK 310 can be used to generate a message authentication code MAC)*; and

using a hashing function at the electronic communication apparatus to compute a Hashed Method Authentication Code (HMAC) on the message *(Quick: par. 0038; HMAC-SHA-1 scheme; HMAC is implemented in the subscriber identification token)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Quick with that of SyncML and Lahteenmaki wherein generating, at the server, an integrity key; sending the integrity key to the electronic communication apparatus; using the integrity key at the electronic communication apparatus to generate MAC values; and using a hashing function at the electronic communication apparatus to compute a Hashed Method Authentication Code (HMAC) on the message to provide users with a mean for providing secure authentication to a subscriber roaming outside his or her home system *(Quick: par. 0007)*.

SyncML, Lahteenmaki, and Quick disclose all limitations as recited above. SyncML, Lahteenmaki, and Quick do not explicitly disclose the integrity key is encrypted with the public key of the electronic communication apparatus.

However, in an analogous art, Beatson discloses a method for authenticating a digitized signature for execution of an electronic document, wherein the integrity key is encrypted with the public key of the electronic communication apparatus *(Beatson: par.*

0080; the device (server) encrypts the secret key (integrity key) with the public key of the

destination host (electronic communication apparatus) and communicates the data to that

host with the encrypted secret key).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to combine the method and system of Beatson with that of

SyncML, Lahteenmaki, and Quick, wherein the integrity key is encrypted with the public

key of the electronic communication apparatus to provide users with a means for providing

authenticating access to an electronic system *(Beatson: par. 0003).*

Conclusion

17.   Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner

can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information

for unpublished applications is available through Private PAIR only. For more information

about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on

access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-

217-9197 (toll-free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-9199 (IN USA

OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437